IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
Before the Board of Patent Appeals and Interferences

In re Patent Application of	Conf. No.: 8934
ROXBURGH, et al.	Atty. Ref.: LB -36-2015
Serial No. 10/594,124	TC/A.U.: 2165
Filed: September 25, 2006	Examiner: Bai D. Vu

For: METHOD AND APPARATUS FOR COMMUNICATING DATA BETWEEN COMPUTER DEVICES

* * * * * * * * * * *

November 1, 2010

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

REPLY BRIEF

Appellant hereby submits this Reply brief under the provisions of 37 C.F.R. 1.193(b) in response to the Examiner's Answer mailed August 31, 2010.

The arguments set forth in the Appeal Brief dated June 15, 2010 are incorporated herein by reference, and Appellant will not repeat the same herein. The following arguments are presented in response to new arguments presented in the Examiner's Answer and to further clarify Appellant's previous positions.

1. First Reply Argument

With respect to the issue of whether claims 16 and 17 are unpatentable under Section 103(a) over Grantges, Jr. et al. (US 6,510,464) in view of Wilding (US

2005/0050329), and more specifically, with respect to the issue of whether Grantges, Jr./Wilding teaches "the *gateway* including notification means for *initiating* an unauthenticated and unencrypted connection to one or more of the application hosting sub-systems and transmitting over this or each such connection a notification for notifying said one or more of the application hosting sub-systems that *it should initiate a secure authenticated connection with the gateway when the notification means is requested so to do by any one of the services offered by the first sub-system*", emphasis added, the Examiner first stated that the connection between the gateway and the application hosting subsystem is already established and (apparently) secured, see p. 15 of the Examiner's Answer.

Next, the Examiner basically repeated his arguments offered in the Final Office Action of November 19, 2009, alleging that Wilding teaches the above feature, admittedly not explicitly disclosed by Grantges, Jr., by saying that the feature corresponds to the "process starting from the step of transmitting Temporary Server Public Key (i.e., interpreted as a notification to verify the authenticated information) from the service gateway 110 to the service client 108 (i.e., interpreted as hosting sub-system) using unsecure connection, until the step of establishing secure, authenticated and encrypted connection between the service gateway 110 and the service client 108", see p. 17 of the Examiner's Answer.

Claims 16 and 17 do not merely recite sending a transmission from the gateway to an application hosting sub-system, i.e., the service gateway 110 in Wilding sending a Temporary Server Public Key to the service client 108, to establish a secure connection

between the service gateway and the service client. Rather, the invention of claims 16 and 17 requires (i) the gateway (via its notification means) to initiate the connection between the service gateway and the service client and transmit the notification towards the application hosting sub-system (ii) this event occurring when the notification means is requested to do so by one of the services offered by the first sub-system hosting the various services offered to the various application hosting sub-systems.

Wilding fails to teach or suggest (i) or (ii).

Regarding point (i), the connection between the service gateway and the service client is initiated by the customer system. All the encryption packages being sent back and forth between the customer and the service gateway are sent over the TCP connection initiated by the customer system. Paragraph [0028] of Wilding recites "Once the customer has registered with the server, a remote service session can be established. Referring to FIGS. 3A-3B, a flow chart illustrating the steps for establishing a remote session is shown. In step 302, the customer system initiates a connection. The service client 108 establishes a Transmission Control Protocol/Internet Protocol (TCP/IP) connection, or session, to the service gateway 110".

Regarding point (ii), the sending of a Temporary Server Public Key to the service client 108 by the service gateway 110, is not done is response to a request by one of the services in the service gateway. Rather, the sending of this signal is in response to an initiation signal sent by the customer user. Wilding (and Grantges, Jr.) adheres to a classic client/server model where servers simply respond to an input request from a client. In contrast, the invention of claims 16 and 17, enables a plurality of services (255,

256, 257) to offer their services in a secure manner, with the ability to notify their clients (110, 120, 130, 140, 150) when necessary – and all of this is done in an efficient manner, by requesting the notification means to send a notification to the clients to contact the server. In this way, the services do not need to worry themselves about how to implement either the security requirements or the notifications, since this is all handled centrally by the gateway layer (200 – especially 220) and the clients do not need any complex functionality to allow a connection to be set up by a third party in a secure manner.

It is noted that in the invention of claims 16 and 17, even though an application hosting sub-system may initiate a secure and authenticated connection to the gateway, it is the notification means of the gateway that initiates the transmission of the notification in response to a request by one of the services offered by the first sub-system of the gateway. This is not taught or suggested by Grantges, Jr./Wilding.

The cited portion of Grantges (col. 4, lines 7-19), see p. 4 of the Examiner's Answer, actually amply demonstrates that Grantges is a conventional system in which the client initiates all connections with the server system.

Moreover, Appellant points out that just because the feature of "the gateway and each application hosting sub-system being arranged to permit each application hosting sub-system to initiate a secure and authenticated connection" appears before the feature of "the gateway including notification means for initiating an unauthenticated and unencrypted connection to one or more application hosting sub-systems" in the claim

language (see p. 15 of the Examiner's Answer), this does not mean that an authenticated connection is in place when an unauthenticated connection is initiated.

It is of course known for secure connections to be set up after initiation by a client device to a server device, and therefore this feature appears in the claim before the novel feature of a notification means arranged to initiate a new unauthenticated and unencrypted connection (when there is no secure connection already in place). In the method according to claims 16 and 17, naturally, the initiation of an unauthenticated unencrypted connection by the notification means to the application hosting sub-system occurs before the application hosting sub-systems initiates a secure connection to the gateway. Indeed the reason that the application hosting sub-system initiates such a secure connection is precisely because **it has been told to do so** in the notification received from the notification means via the unsecure connection initiated by the notification means!

Moreover, Appellant submits that the "options page" of Grantges, Jr., identified by the Examiner as the notification sent by the gateway, see p. 16 of the Examiner's Answer, does not read on a notification sent to a client to initiate a secure authenticated connection with the gateway in response to a request by one of the services offered by the first sub-system. First, the "options page" comprises a list of applications 24_1, 24_2...of the first sub-system for selection by the user 18 of the client computer 22 (col. 9, lines 19-24 in Grantges, Jr.). Second, this "options page" is not sent due to a request by one of the services of the server.

Finally, the Examiner stated that "As it is well known in the telecommunication technology, all 'communicating' devices in a network send a pulse/beat to each other to make sure of the availability for further communication therefore the 'options list' devices are established devices that share the same communication network", see p. 16 of the Examiner's Answer.

Claims 16 and 17 do not merely recite an "acknowledgment" or "availability" transmission but rather they specifically require "a notification for notifying said one or more of the application hosting sub-systems that it should initiate a secure authenticated connection with the gateway when the notification means is requested so to do by any one of the services offered by the first sub-system". This is not disclosed or suggested by the cited prior art.

2. Second Reply Argument

With respect to the issue of whether dependent claim 5 is unpatentable under Section 103(a) over Grantges, Jr. et al. (US 6,510,464) in view of Wilding (US 2005/0050329) and further in view of Osterman (US 5,935,211), and more specifically, with respect to the issue of whether Osterman teaches that the notification means specifies the number of times up to a specified number a notification to an application hosting sub-system is to be sent in case of failure to deliver the notification, the Examiner basically repeated his rejection argument presented in the Final Office Action of November 19, 2009, see p. 13 of the Examiner's Answer.

As discussed in the Appeal Brief of June 15, 2010, Osterman merely teaches removing inactive processes of the client from the notification list, not specifying the

number of times which a notification is to be retried in the event of failure to deliver the notification. This has not been rebutted by the Examiner in the Examiner's Answer.

For at least the reasons set forth above and discussed in detail in the previously-filed Appeal Brief, it is respectfully requested that the rejections on appeal be reversed.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: /Leonidas Boutsikaris/
Leonidas Boutsikaris
Reg. No. 61,377

LB:
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100